

JUL 09 2008

Amendment Dated July 9, 2008
Serial No. 10/615,513

REMARKS

Reconsideration of the rejections set forth in the Office Action dated January 10, 2008 is respectfully requested. By this amendment claims 1 and 14 have been amended. Currently, claims 1-7, 9-11, and 13-25 are pending in this application.

Rejection under 35 USC 103

Claims 1-3, 7, 9-11, 13-15, 17-18, and 21-22 were rejected under 35 USC 103 as unpatentable over Hamilton (U.S. Patent No. 7,123,974) in view of Daniely (U.S. Patent No. 6,763,469). Claims 4-6 and 23-25 were rejected under 35 USC 103 as unpatentable over Hamilton in view of Daniely, and further in view of Danner (U.S. Patent No. 7,194,003). These rejections are respectfully traversed in view of the amendments to the claims and the following arguments.

This application relates to industrial networks, and more particularly to a way in which access to particular PLCs and attendant factory machines may be circumscribed so that only particular authorized individuals may have access to particular PLCs over the industrial network.

As discussed in the background of the specification, for example at page 1, PLCs are able to be connected to a company's Ethernet network or other data network. However, where there is more than one person that is allowed to program PLCs on the network, a person may accidentally make a change to the wrong PLC or a person may intentionally change the programs of PLCs on the network to affect operation of the machines associated with the PLCs.

Accordingly, applicants proposed to implement a security point (Secure Policy Implementation Point – SPIP) between the network and the PLC to control who is allowed to access particular PLCs via the network. Thus, simply obtaining access to a centralized network controller is insufficient to program all PLCs connected to the network – the SPIP will also require that the user of the network control system be authenticated and authorized at a particular SPIP before allowing the user to make changes to the PLCs associated with the SPIP.

The Examiner cited Hamilton as teaching a local area network interconnecting programmable logic controllers on the network. (See Office Action at page 2). The Examiner contends that Hamilton teaches a Security Policy Implementation Point (SPIP) between the network and the programmable logic controllers. *Id.* As support for this position, the Examiner has cited Hamilton at Figs. 1, 2, and 6, and more particularly Fig. 6, col. 9, lines 7-33.

Amendment Dated July 9, 2008
Serial No. 10/615,513

In Fig. 6, and the associated text at Col. 9, lines 7-33, Hamilton shows a system 500 illustrating security operations. In the second sentence of the paragraph (Col. 9, lines 8-9), Hamilton states that the "access tool 510" has one or more security layers 520. In Hamilton, the term "access tool" is used to refer to the management program that is used to interact with the PLCs on the network (see Col. 4, lines 60-61). Thus, Fig. 6 and the text at col. 9, lines 7-33 is unrelated to a SPIP, but rather teaches that the management tool that is used to interact with the PLCs should have one or more security layers. Accordingly, applicants respectfully traverse the Examiner's interpretation of Fig. 6 and col. 9, lines 7-33 of Hamilton as showing a SPIP that is configured to participate in VPN on the industrial network.

On page 3 of the Office Action the Examiner further cited col. 10, lines 45-60 of Hamilton as providing support for the position that Hamilton teaches a SPIP connected between the network and the PLCs. At Col. 10, lines 45-60, Hamilton teaches that applications can communicate with the PLCs, and control the PLCs. This relates to how PLCs can be controlled on the network. This portion of Hamilton does not teach or suggest a SPIP interposed between the PLC and the network. Accordingly, applicants respectfully traverse the Examiner's interpretation of Col. 10, lines 45-60 as showing a SPIP connected between the network and the one or more PLCs which provides authentication, authorization, and/or other security measures when communicating activity data over a network.

Applicants note, in this regard, that the term "activity data" in Hamilton, is data that is related to a record of interactions with the PLCs. (see Col. 5, lines 4-23). Hamilton is focused on recording what takes place with the PLCs, and the data that is collected in connection with this is referred to as activity data. While this data may be protected as noted by the Examiner, the protection of the activity data is unrelated to protecting access to the PLC in the first instance.

The Examiner cited Daniely as teaching a SPIP connected between the local area network and one or more components. Daniely shows a security system in which a local security device is used to protect each computer connected to the network. For example, in Fig. 1A of Daniely, a local security device 20 is connected between each computer 22 and the network. The local security device is used to control what a user (using the computer) can do on the network. (Daniely at Col. 4, lines 1-12). Daniely defines the term "computer" to include personal computers or other devices that have an operating system such as a DOS, Windows, Linux, or other operating system (Daniely at Col. 3, lines 9-29). Thus, Daniely is not related to protecting

Amendment Dated July 9, 2008
Serial No. 10/615,513

PLCs on the networks, but rather shows that each computer on a computer network (such as the computer running a PLC management program) may have a local security device to control its actions on the network and to control which other computers on the network have access to it. (See e.g. Daniely at Col. 6, lines 24-52).

Accordingly, if applicants understand correctly, Hamilton shows an industrial network that has an access tool for controlling PLCs, and shows that interactions with the PLCs should be logged. Hamilton further teaches that the access tool, not the PLCs, should implement local security. Daniely shows a standard computer network in which the computers connected to the network all are provided with a local security device. Once again, in Daniely (like Hamilton) the computers, not PLCs, are being provided with local security.

The Examiner has taken the position that it would have been obvious to combine these two references, because doing so would have enabled flexible network security at the local level, to protect the computer/device from unauthorized access and permit authorized access within an organization.

Applicants respectfully traverse this conclusion. Hamilton teaches an access tool that has access to all PLCs, and teaches that the access tool should have local security. Daniely teaches protecting individual computers, but does not relate to protecting PLCs. Accordingly, combining Daniely with Hamilton would have taught that the computer in Hamilton that is running the access tool should be provided with a security system that is dedicated to that computer. However, since neither Hamilton nor Daniely teach or suggest providing PLCs with local protection, the combination of Hamilton and Daniely would not have suggested the use of a SPIP between particular sets of PLCs and the industrial network as claimed. Accordingly, applicants respectfully request that the rejection under 35 USC 103 over Hamilton and Daniely be withdrawn.

Conclusion

Applicants believe that the claims submitted in this case are patentable over the cited references, even when the claims are given their broadest reasonable interpretation. However, applicants are interested in working with the Examiner to define claims of appropriate scope that both the Examiner and applicants believe are patentable over the art of record. In connection with this, applicants would welcome an opportunity to discuss this case with the Examiner and

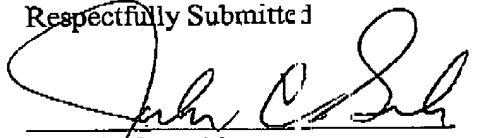
Amendment Dated July 9, 2008
Serial No. 10/615,513

JUL 09 2008

cordially invite the Examiner to call applicant's representative if the Examiner feels that a telephone interview would further prosecution of this application. Likewise, if the Examiner has any other concerns about any of the statements made herein, the Examiner is invited to telephone applicants representative to discuss these matters.

If any fees are due in connection with this filing, the Commissioner is hereby authorized to charge payment of the fees associated with this communication or credit any overpayment to Deposit Account No. 502246 (Ref: NN-15929).

Respectfully Submitted


John C. Gorecki
Registration No. 38,471

Dated: July 9, 2008

John C. Gorecki, Esq.
P.O. Box 553
Carlisle, MA 01741
Tel: (978) 371-3218
Fax: (978) 371-3219
john@gorecki.us